

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-240691

(43) 公開日 平成10年(1998) 9月11日

(51) Int.Cl.⁹

G 0 6 F 15/00

識別記号

3 3 0

F I

G 0 6 F 15/00

3 3 0 F

3 3 0 G

A 6 1 B 3/10

A 6 1 B 3/10

Z

5/117

5/10

3 2 0 A

G 0 6 F 17/60

G 0 6 F 15/21

3 4 0 B

審査請求 未請求 請求項の数 7 F D (全 13 頁) 最終頁に続く

(21) 出願番号

特願平9-59861

(22) 出願日

平成9年(1997) 2月26日

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 星野 恭祐

東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

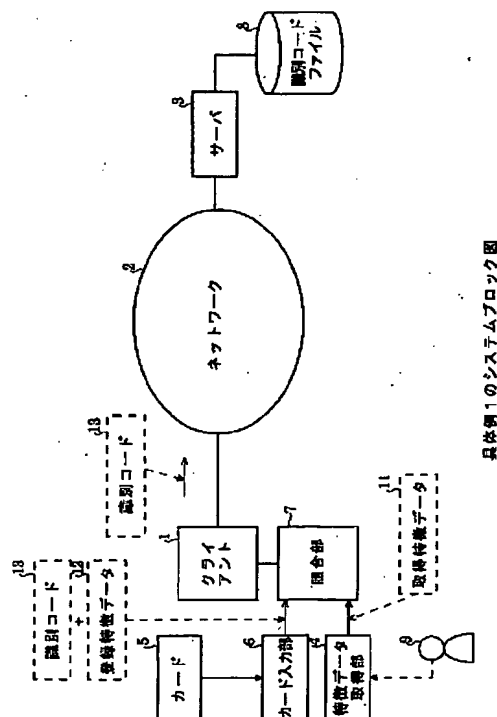
(74) 代理人 弁理士 佐藤 幸男 (外1名)

(54) 【発明の名称】 ネットワークセキュリティシステム

(57) 【要約】

【解決手段】 特徴データ取得部4は、ユーザー9の眼の映像から特徴データを取得する。カード5には、予めユーザー本人の登録特徴データが格納されている。照合部7でユーザー9がカード所有者本人と確認されると、カード5に格納された識別コードがクライアント1からサーバ3に送られる。サーバ3は、この識別コードに基づいてクライアント1にサービスを提供する。

【効果】 ネットワーク2を特徴データや暗証番号等が流れないため個人情報の漏洩のおそれがなく、本人以外がサービスにアクセスできないため安全を確保できる。



【特許請求の範囲】

【請求項1】 クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録された登録特徴データと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取った登録特徴データと特徴データ取得部が取得したユーザーの眼の映像の特徴データとを照合して、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、サーバ側には、正規のユーザーの識別コードを格納した識別コードファイルを備え、クライアント側で前記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。

【請求項2】 クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録されたファイル検索キーと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取ったファイル検索キーにより登録特徴データファイルからカード所有者の登録特徴データを読み出すとともに、前記特徴データ取得部が取得したユーザーの眼の映像の特徴データとを照合して、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、サーバ側には、正規のユーザーの識別コードを格納した識別コードファイルを備え、クライアント側で前記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。

【請求項3】 クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録されたファイル検索キーと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取ったファイル検索キーにより、クライアントに対してネットワークを介して接続された登録特徴データファイルから、カード所有者の登録特徴データを読み

出して、前記特徴データ取得部が取得したユーザーの眼の映像の特徴データと照合し、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、サーバ側には、正規のユーザーの識別コードを格納した識別コードファイルを備え、クライアント側で前記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。

【請求項4】 請求項1から3のいずれか1項において、

サーバは、クライアントに対して、照合処理の開始を要求してからその結果の通知を受けるまでの時間を監視して、その時間が妥当な時間範囲外である場合に、不正処理と判断することを特徴とするネットワークセキュリティシステム。

【請求項5】 クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像を取得するカメラを備え、サーバ側には、ネットワークを通じてクライアントから受信した眼の映像のビットマップデータから特徴データを取得し、この特徴データと、予め正規のユーザーから取得した登録特徴データファイルを参照して得た登録特徴データとを照合し、ユーザーがカード所有者本人かどうかの確認を行う照合部を備えたことを特徴とするネットワークセキュリティシステム。

【請求項6】 請求項5において、クライアント側から入力された識別コードをネットワーク介してサーバが受信し、この識別コードを用いて登録特徴データファイルから該当する登録特徴データもしくは登録特徴データ群を読み出して、照合部による照合対象とすることを特徴とするネットワークセキュリティシステム。

【請求項7】 クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録された登録特徴データとユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取った登録特徴データを用いてユーザーがカード所有者本人かどうかの確認を行う照合部とを備え、サーバ側には、正規のユーザーの識別コードと登録特徴データもしくは登録特徴データ群とを対応させて格納した登録特徴データファイルを備え、クライアントで読み込んだ識別コードがサーバに送信されると、サーバでは、登録特徴データファイルを参照し

て、対応する登録特徴データもしくは登録特徴データ群を得てクライアントに送信し、

クライアントの照合部は、サーバから受信した登録特徴データもしくは登録特徴データ群と、前記カード入力部が読み取った登録特徴データと、特徴データ取得部が取得したユーザーの眼の映像の特徴データとを相互に照合して、ユーザーがカード所有者本人かどうかの確認を行い、

前記照合処理の結果、ユーザーがカード所有者本人と確認したとき、その旨がクライアントからサーバに通知され、

サーバでは、その通知に基づいてサービスを開始することを特徴とするネットワークセキュリティシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークを通じて決裁等を行う場合の安全を確保するネットワークセキュリティシステムに関する。

【0002】

【従来の技術】マルチメディアパソコンと呼ばれるパーソナルコンピュータは、音声や画像等を扱うことができ、電子メールその他各種の情報送受信に広く利用されている。また、インターネットに代表されるような巨大なネットワークには、このような端末を接続し、商取引を含む様々なサービスが提供されている。このようなネットワークを通じた取引を行う場合、取引を成立させるために所定の決裁が必要となる。しかしながら、ネットワーク上をパスワードやキャッシュカードのコードデータ等を伝送した場合に、いわゆるハッカー等によりそのデータが盗まれて悪用されるおそれがある。従って、一般には決裁は申込用紙の郵送や銀行の窓口における振込処理等で実行されている。

【0003】

【発明が解決しようとする課題】しかしながら、従来のような決裁の方法は、ユーザーにとって煩わしいことからネットワークを用いた取引の利便性に欠ける。こうした点を解決するため、暗号化技術が広く研究されている。これでも必ずしもハッカーに対し完全な防御がなされとは限らない。

【0004】一方、例えば入場者管理等のために、眼の映像から取得される特徴データを利用して、本人を確認する技術が開発されている（特公平5-84166号公報）。ここでは、眼の映像の一部であるアイリスデータを処理した所定の特徴データを得て、指紋等と同様にして本人であるかどうかの判断をしている。この種の技術をネットワークにおける取引の安全確保に利用することが好ましい。

【0005】

【課題を解決するための手段】本発明は以上の点を解決するため次の構成を採用する。

10

〈構成1〉クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録された登録特徴データと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取った登録特徴データと特徴データ取得部が取得したユーザーの眼の映像の特徴データとを照合して、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、サーバ側には、正規のユーザーの識別コードを格納した識別コードファイルを備え、クライアント側で上記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。

20

【0006】〈構成2〉クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録されたファイル検索キーと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取ったファイル検索キーにより登録特徴データファイルからカード所有者の登録特徴データを読み出すとともに、上記特徴データ取得部が取得したユーザーの眼の映像の特徴データとを照合して、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、サーバ側には、正規のユーザーの識別コードを格納した識別コードファイルを備え、クライアント側で上記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。

30

40

【0007】〈構成3〉クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録されたファイル検索キーと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取ったファイル検索キーにより、クライアントに対してネットワークを介して接続された登録特徴データファイルから、カード所有者の登録特徴データを読み出して、上記特徴データ取得部が取得したユーザーの眼の映像の特徴データと照合し、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、サーバ側には、正規のユーザーの識別コードを格納した識別コー

50

ドファイルを備え、クライアント側で上記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。

【0008】〈構成4〉構成1から3のいずれか1項において、サーバは、クライアントに対して、照合処理の開始を要求してからその結果の通知を受けるまでの時間を監視して、その時間が妥当な時間範囲外である場合に、不正処理と判断することを特徴とするネットワークセキュリティシステム。

【0009】〈構成5〉クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像を取得するカメラを備え、サーバ側には、ネットワークを通じてクライアントから受信した眼の映像のビットマップデータから特徴データを取得し、この特徴データと、予め正規のユーザーから取得した登録特徴データファイルを参照して得た登録特徴データとを照合し、ユーザーがカード所有者本人かどうかの確認を行う照合部を備えたことを特徴とするネットワークセキュリティシステム。

【0010】〈構成6〉構成5において、クライアント側から入力された識別コードをネットワーク介してサーバが受信し、この識別コードを用いて登録特徴データファイルから該当する登録特徴データもしくは登録特徴データ群を読み出して、照合部による照合対象とすることを特徴とするネットワークセキュリティシステム。

【0011】〈構成7〉クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録された登録特徴データとユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取った登録特徴データを用いてユーザーがカード所有者本人かどうかの確認を行う照合部とを備え、サーバ側には、正規のユーザーの識別コードと登録特徴データもしくは登録特徴データ群とを対応させて格納した登録特徴データファイルを備え、クライアントで読み込んだ識別コードがサーバに送信されると、サーバでは、登録特徴データファイルを参照して、対応する登録特徴データもしくは登録特徴データ群を得てクライアントに送信し、クライアントの照合部は、サーバから受信した登録特徴データもしくは登録特徴データ群と、上記カード入力部が読み取った登録特徴データと、特徴データ取得部が取得したユーザーの眼の映像の特徴データとを相互に照合して、ユーザーがカード所有者本人かどうかの確認を行い、上記照合処理の結果、ユーザーがカード所

有者本人と確認したとき、その旨がクライアントからサーバに通知され、サーバでは、その通知に基づいてサービスを開始することを特徴とするネットワークセキュリティシステム。

【0012】

【発明の実施の形態】以下、本発明の実施の形態を具体例を用いて説明する。

〈具体例1〉図1は、具体例1のシステムを示すブロック図である。このシステムのクライアント1がネットワーク2を介してサーバ3に接続され、クライアント1を操作するユーザーがサーバ3の各種のサービスを受ける構成となっている。クライアント1もサーバ3も例えばパーソナルコンピュータやワークステーションにより構成される。クライアント1には、特徴データ取得部4、カード入力部6、照合部7が接続されている。特徴データ取得部4は、ユーザー9の眼の映像を図示しないカメラ等で撮影し、既に説明したようなアイリスデータあるいはその他の眼の各部の特徴をデータ化した特徴データを取得する部分である。カード入力部6は、磁気カードやICカードのようなカード5を装着することによって、その中に記憶されたデータを読み込むための装置である。

【0013】カード5には、ユーザー9が予め登録した登録特徴データ12と、ユーザー9の取引に使用される識別コード13が格納されている。照合部7は、特徴データ取得部4から入力する取得特徴データ11と、カード入力部6から入力する登録特徴データ12とを比較照合して、ユーザー9が本人のカード5を使用しているかどうかを判断する部分である。本人と判断された場合に、照合部7は、カード入力部6から受け入れた識別コード13をクライアント1に出力する構成となっている。識別コード13はネットワーク2を通じてサーバ3に送られる。

【0014】サーバ3はクライアント1から送られた識別コードを受信して、識別コードファイル8を参照し、所定のサービス提供のためのアクセス処理等を許可する装置である。このサーバ3にアクセスを許可された場合、ユーザー9は所定の取引処理を実行しあるいは各種のサービスを受けて所定の決裁を実行することができる。なお、サーバ3は、識別コードを受け入れた場合に識別コードファイル8に格納されたデータを読み出し、ユーザー9に関する情報を取得し、その情報に基づいて各種のサービスを行う。また、必要に応じてクライアント1側にユーザーの情報を送り、ユーザー9による確認処理等を行うこともできる。

【0015】図2には、具体例1のシステム動作フローチャートを示す。この図によって、図1に示した具体例1のシステムの動作を説明する。まず、ステップS1において、クライアント1からサーバ3に対しアクセス要求が行われると、サーバ3はこれに対して特徴データの

照合要求を行う。

【0016】次に、ステップS2において、クライアント1が特徴データ取得部4を動作させてユーザー9の眼の映像を取得する。そして、所定の処理により特徴データを取得する。更に、ステップS3において、カード5から登録特徴データ12を読み取る。次に、ステップS4において、照合部7は、照合処理を行う。ステップS5において、カードの所持者が本人であると確認されるとステップS6に進み、カードから読み取った識別コードをサーバ3へ送信する。サーバ3はこれを受信し、ステップS7において、識別コードファイル8を参照し、所定のユーザーに対する情報や属性データ等を得る。こうして、サーバ3はクライアント1にアクセスを許可しサービスを開始する。

【0017】なお、ステップS5において、本人でないと確認された場合はステップS8に進み、処理を中止する。ここで、クライアント1に対し、再度眼の映像の入力あるいはカードの投入を要求するようにしてもよい。

【0018】〈具体例1の効果〉この例によれば、クライアント側でアイリスデータのような眼の映像の特徴データを使用して本人確認を行うため、第三者の利用を阻止し、セキュリティが高められる。しかも、ネットワークに流れるデータはサーバ3からの要求とその応答である識別コード13のみのため、特徴データや暗証番号のような個人情報をネットワークに流すことはない。このため、個人情報漏洩による悪用を防止できる。しかも、ユーザー本人は知ることのできないような識別コードを利用することによって、識別コードが他人に盗まれる危険も減少し、商取引のセキュリティを向上させる。

【0019】〈具体例2〉図3に、具体例2のシステムブロック図を示す。このシステムも、クライアント1がネットワーク2を介してサーバ3に対し所定のアクセス要求を行う構成となっている。クライアント1に接続された特徴データ取得部4、カード入力部6、照合部7等の構成は具体例1と同様である。この具体例2では、新たに登録特徴データファイル15が照合部7に接続される。登録特徴データファイル15には、所定のファイル検索キー14と登録特徴データ12とが対応付けられて格納されている。

【0020】また、カード5には、このファイル検索キー14と識別コード13とが格納される。照合部7は、ファイル検索キー14を使用して登録特徴データファイル15を検索し、対応する登録特徴データ12を読み出す。そして、その登録特徴データ12と特徴データ取得部4から入力する取得特徴データ11との照合処理を行うように構成されている。その他の構成は具体例1と同様である。

【0021】図4を用いて、具体例2の動作を説明する。図4は、具体例2のシステム動作フローチャートである。図のステップS1では、具体例1と同様、クライ

アントからのアクセス要求に対しサーバが特徴データの照合要求を行い、ステップS2ではクライアントがユーザーの眼の映像を取得する。次に、ステップS3では、ユーザー9が投入したカード5からファイル検索キー14を読み込む。ステップS4で、照合部7は登録特徴データファイル15を参照して、ファイル検索キー14に対応する登録特徴データ12を読み出す。そして、ステップS5において、特徴データ取得部4から入力した取得特徴データ11との照合処理を行う。この照合の結果、本人と判断されると、ステップS6からステップS7に進み、識別コード13をサーバ3へ送信する。以下の処理は具体例1と同様で、ステップS8ではサーバが識別コードを用いたサービスを開始する。本人と判断されなければ処理が中止される（ステップS9）。

【0022】〈具体例2の効果〉具体例1と比較すると、カード5に登録特徴データを格納せず、ファイル検索キーを格納するようにしたので、カード5に格納すべきデータ量を十分に少なくできる。従って、簡単な磁気カード等でカードを実現することができ、取引コストを削減できる。その他の効果は具体例1と同様である。

【0023】〈具体例3〉図5に、具体例3のシステムブロック図を示す。この図に示すように、具体例3では、登録特徴データファイル15をクライアント1に対し第1ネットワーク2Aを介して接続している。この第1ネットワーク2Aは、例えばLAN（ローカルエリアネットワーク）のような、ネットワーク上のデータの秘密を確保しやすいネットワークとする。この第1ネットワーク2Aには、図示しない他のクライアントが多数接続されているものとする。また、登録特徴データファイル15には、ファイル検索キー14と登録特徴データ群18とが格納されている。

【0024】図3に示した具体例2のシステムとこの具体例3のシステムとを比較すると、登録特徴データファイル15がクライアント1に対し第1ネットワーク2Aを介して接続されている点のみが異なる。なお、登録特徴データファイル15に格納されたファイル検索キー14に対応する登録特徴データ群18は、登録特徴データ全体を適当に分割した登録特徴データの集合である。

【0025】照合部7は照合処理を行う場合、クライアントと第1ネットワーク2Aを通じて登録特徴データファイル15を検索し、必要な登録特徴データ群18を取得する。その後、照合処理を実行する。その他の動作は図3に示すものと全く同一である。図3に示した具体例2に示すように、ファイル検索キーと登録特徴データとを一对一对応させてもよい。また逆に、具体例2の場合にも、ファイル検索キー14に対応させて登録特徴データ群を格納してもよい。この場合、照合部7は登録特徴データ群の中に取得特徴データ11と一致するものがあるかどうかを判断することになる。具体例3においても同様で、照合部7は第1ネットワーク2Aを通じて受

け入れた登録特徴データ群18と取得特徴データ11との照合処理を行う。1個のファイル検索キーで複数の登録特徴データを取り出すのは、全ての登録特徴データに対応するファイル検索キーを用意するとファイル検索キーの文字数が著しく増加して管理が容易でなくなるからである。また、照合処理が比較的速やかにできる程度に登録特徴データを取り出せば、後は照合部7によって照合処理を行えばよいからである。

【0026】〈具体例3の効果〉具体例2の効果に加えて、登録特徴データファイル15が第1ネットワーク2Aに接続されているため、この第1ネットワーク2Aに接続された他のクライアントも自由にこの登録特徴データファイル15を参照できる。従って、クライアント側に大きな登録特徴データファイルを保存しておく必要がなくなる。もちろん、登録特徴データファイル15は1つでなく、任意の数だけ第1ネットワーク2Aに接続されても構わない。これによって、クライアント側に特徴データの照合部さえあれば自由にネットワークと接続しシステムの拡張が可能になる。また、登録特徴データファイル15の増減変更が容易にできるためメンテナンス性が向上し、維持コストが削減できる。

【0027】〈具体例4〉図6には、具体例4のシーケンスチャートを示す。この具体例4では、サーバがクライアントからアクセス要求を受けた場合に、クライアントが実際に特徴データの照合処理を実行しているかどうかを監視し、その処理時間等から不正な処理を排除する。この具体例4を適用するシステムは、図1、図3、図5等により説明されたどのシステムであってもよい。

【0028】図6において、まずステップS1で、クライアント1がサーバ3に対しアクセスを要求する。サーバ3はこれに対応してステップS2でクライアント1に対し特徴データの照合要求を行う。クライアント1はステップS3において、その照合準備を行う。即ち、例えば図1のシステムでは、ユーザー9の眼の映像を特徴データ取得部4が取得し、特徴データの生成処理を行う。次に、ステップS5において、サーバ3に対し準備完了報告を行う。一方、サーバ3はステップS2でクライアント1に対し特徴データの照合要求を行った後、タイマによる監視を行う(ステップS4)。

【0029】即ち、照合要求から準備完了報告までの時間を監視し、クライアント1の側で適切な処理を行った後に準備完了報告S5が受け入れられたかどうかを判断する。著しく報告までの時間が長い場合や異常に短い場合には何らかの不正が生じたとして取引を停止する。不正を検出した場合にはステップS10に進み、取引停止処理等を行う。更に、ステップS5で準備完了報告を受けたサーバ3は、ステップS6で照合スタート指示を行う。これに対しクライアント1は、ステップS7において照合処理を実行し、ステップS9において結果通知を報告する。サーバ3は、この場合にも照合スタート指示

S6をクライアント1に送った時点から結果通知をステップS9で受信するまでタイマ監視を行う(ステップS8)。

【0030】ここでも、必要な照合処理のための時間を考慮し、著しく短い場合と著しく長い場合とを不正処理と判定する。このようにして、実際の特徴データ照合処理を行っているか、この処理を行わずに例えば識別コードを直ちに送信してきているか等を区別することができる。

10 【0031】〈具体例4の効果〉以上のように、クライアントによる照合準備等を含む照合処理時間をサーバが監視するので、不正処理を排除してセキュリティを高められる。例えば、予め不正に取得した特徴データを用いてすぐに準備完了報告がきたり、照合処理ができるはずのないような短時間に識別コードが返ってくると、不正に準備されたものと判断できる。

20 【0032】〈具体例5〉図7には、具体例5のシステムブロック図を示す。このシステムもクライアント1がネットワーク2を介してサーバ3に接続されている。また、このシステムでは、クライアント1に対してカメラ16が接続され、ユーザー9の眼の映像を取得する構成となっている。また、サーバ3の側には登録特徴データファイル15及び照合部7が設けられる。

30 【0033】上記の構成のシステムは、次のように動作する。図8には、具体例5の動作フローチャートを示す。図のステップS1において、まずクライアント1からのアクセス要求がサーバ3に到着すると、サーバ3はクライアント1のカメラ16に対し起動要求を行う。ステップS2では、クライアント1がカメラ16を用いてユーザー9の眼の映像を取得し、眼の映像のビットマップデータ17をネットワーク2を通じてサーバ3に送信する。

【0034】ここで、サーバ3では、具体例1や具体例2で実行したクライアント側による眼の映像の特徴データ取得処理をサーバ側で行う(ステップS3)。次に、ステップS4において、サーバ側で登録特徴データファイル15を参照して照合処理を実行する。即ち、サーバ側には眼の映像のビットマップデータが転送され、ここからサーバ側において特徴データを取得し、登録特徴データファイルとの照合が行われる。ステップS5で本人と確認されると、ステップS6で所定のサービスその他の処理が開始される。一方、本人と確認されないとステップS5からステップS7に進み、処理が中止される。

50 【0035】〈具体例5の効果〉ビデオカメラのような撮影機材によってユーザーの眼の映像が直接サーバ側に送られ、サーバ側で特徴データの照合処理等を実行するため、登録特徴データの集中管理が行えるという効果がある。しかも、眼の映像そのものを送信するため、識別データや暗証番号、その他のように簡単に解読できる内容でないためセキュリティの向上が期待できる。また、

一般のマルチメディアパソコンに設けられた簡単なビデオカメラを用いてサーバに対しアクセス要求を実行することができるため、クライアント側の設備費用が安価にできるという効果がある。

【0036】〈具体例6〉図9には、具体例6のシステムブロック図を示す。このシステムは、具体例5の場合と比較すると、クライアント1の側にキーボード21のような入力手段を設け、識別コード13を入力できるようにしている点異なる。その他の部分は具体例5と同様である。

【0037】図10に、具体例6のシステム動作フローチャートを示す。ここでも、具体例5の場合と同様に、ステップS1でクライアントからのアクセス要求に対しカメラが起動し、ステップS2でカメラが撮影した眼の映像をサーバ3へ送信する。サーバ側では、その眼の映像について特徴データを取得する。更に、この具体例6では、ステップS4において、クライアント側で識別コード13をキーボード21を用いて入力する。

【0038】この識別コードはネットワーク2を通じてサーバ3に送られる。サーバ3の照合部7は、登録特徴データファイル15を参照し、識別コード13に対応する登録特徴データ群18を取り出す。その後、この登録特徴データ群18とサーバ3で生成した取得特徴データとの照合処理が行われる。識別コード13と登録特徴データとは、1対1で格納されていてもよいし、登録特徴データ群が1つの識別コード13と対応するように格納されていてもよい。いずれの場合にも、大量の登録特徴データの中から一部の登録特徴データが取り出されて照合処理を行うため、処理時間を短縮できる効果がある。

【0039】〈具体例6の効果〉クライアント側からキーボードを用いて識別コードを入力し、サーバ側での照合対象となる登録特徴データを絞り込むことができるため、照合処理のスピードアップが図られる。また、演算量も少なくなるため、サーバのマシンをローパワーの安価なマシンに置き換えることができるという効果がある。

【0040】〈具体例7〉図11に、具体例7のシステムブロック図を示す。このシステムの構成は、クライアント側とネットワークについては図1に示したシステムと同様である。サーバ3の側には登録特徴データファイル15が設けられ、ここには識別コード13と登録特徴データ12とを対応付けたデータが格納されている。

【0041】図12には、具体例7のシステム動作フローチャートを示す。このシステムは次のように動作する。まず、ステップS1において、クライアントからのアクセス要求に対してサーバが特徴データの照合要求を行う。ステップS2では、クライアントがユーザーの眼

の映像を取得し、ステップS3において、カードから登録特徴データを読み取る。ステップS4では、クライアント側でカードから識別コードを読み取る。そして、ステップS5で、その識別コードをサーバ側に送り、サーバ側で登録特徴データファイル15から識別コードに対応するデータを読み出す。ステップS6では、読み出した登録特徴データをクライアント側に送る。

【0042】即ち、この具体例では、クライアント側にカードから読み出した登録特徴データとサーバで読み出した登録特徴データとが送られ、クライアント側で取得した眼の映像から得た特徴データと3つが同時に照合処理される。ステップS7において、この照合処理を行うと、ステップS8で本人かどうかの判断がなされ、本人と判断されるとステップS9で処理が継続され、本人でないと判断されるとステップS10に進み、処理が中止される。

【0043】〈具体例7の効果〉3種類の特徴データが相互に照合処理されることから、これまでのシステムよりも更に本人確認のためのセキュリティが高まる。

10 【図面の簡単な説明】

【図1】具体例1のシステムブロック図である。

【図2】具体例1のシステム動作フローチャートである。

【図3】具体例2のシステムブロック図である。

【図4】具体例2のシステム動作フローチャートである。

【図5】具体例3のシステムブロック図である。

【図6】具体例4のシーケンスチャートである。

【図7】具体例5のシステムブロック図である。

30 【図8】具体例5のシステム動作フローチャートである。

【図9】具体例6のシステムブロック図である。

【図10】具体例6のシステム動作フローチャートである。

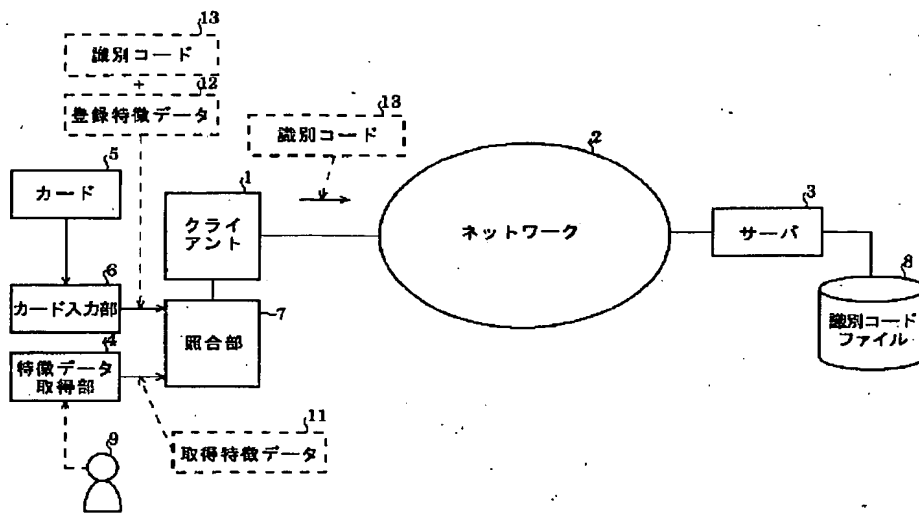
【図11】具体例7のシステムブロック図である。

【図12】具体例7のシステム動作フローチャートである。

【符号の説明】

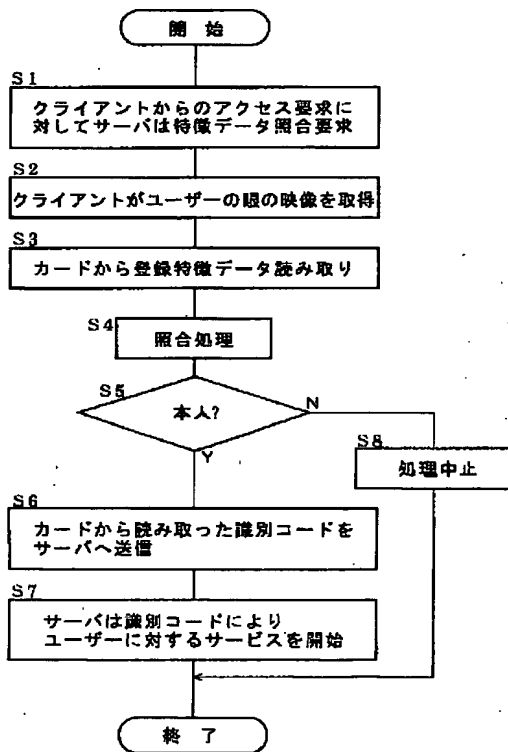
- 1 クライアント
- 2 ネットワーク
- 3 サーバ
- 4 特徴データ取得部
- 5 カード
- 6 カード入力部
- 7 照合部
- 8 識別コードファイル

【図1】



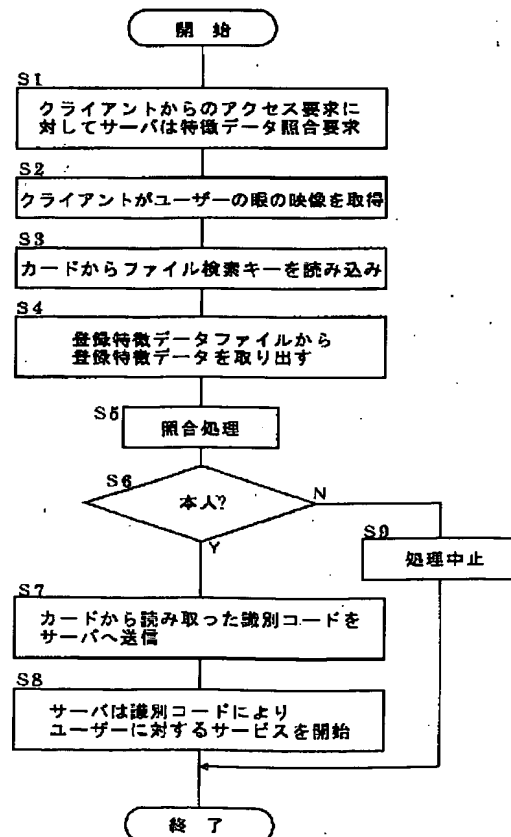
具体例1のシステムブロック図

【図2】



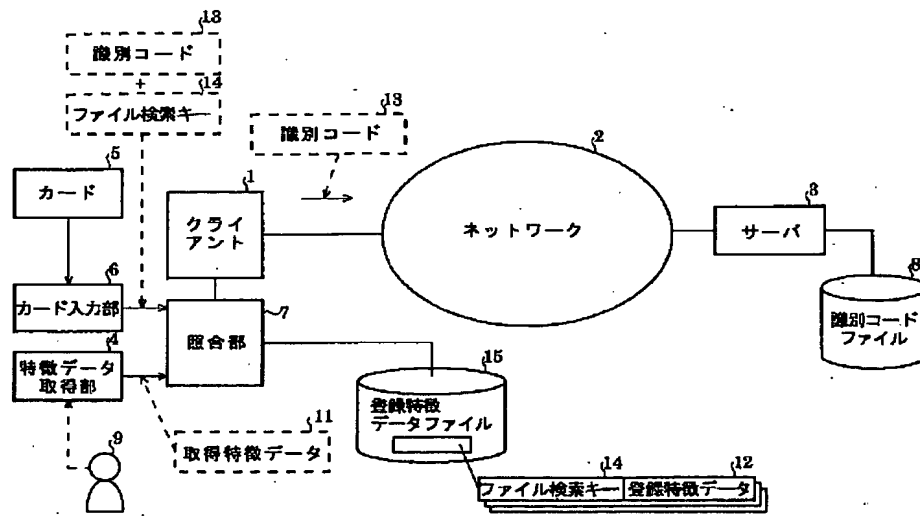
具体例1のシステム動作フローチャート

【図4】



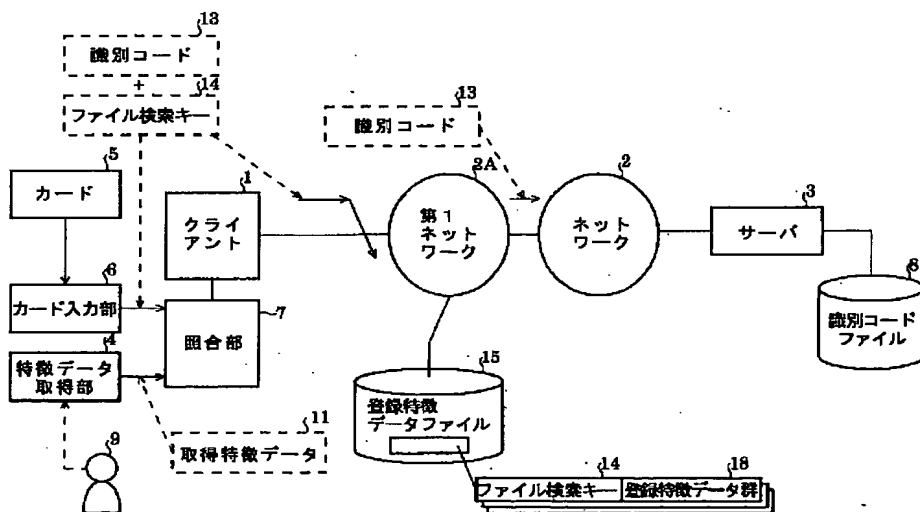
具体例2のシステム動作フローチャート

【図3】



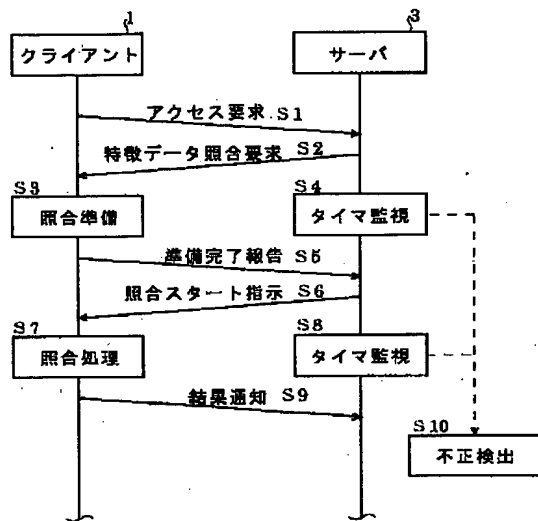
具体例2のシステムブロック図

【図5】



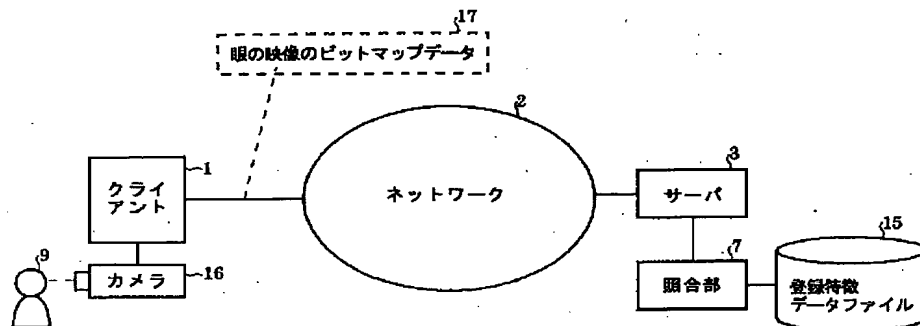
具体例3のシステムブロック図

【図 6】



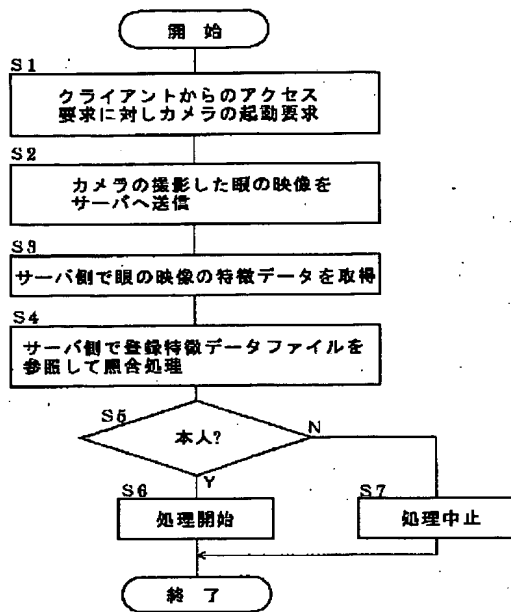
具体例 4 のシーケンスチャート

【図 7】



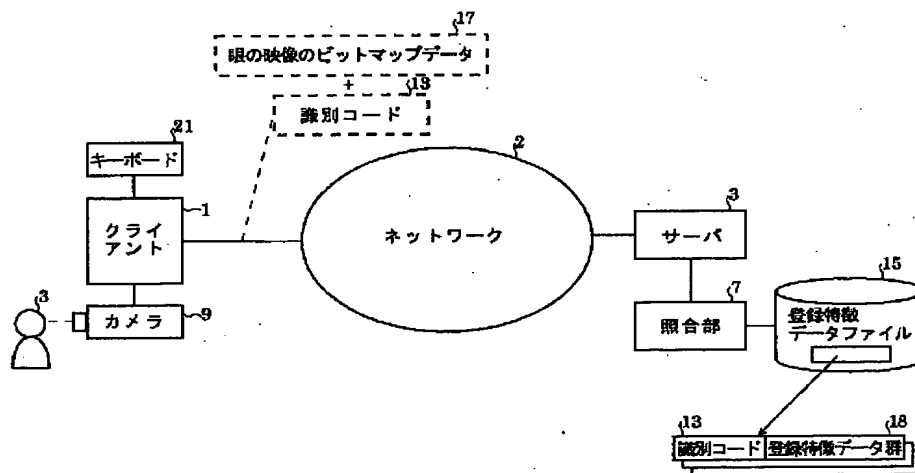
具体例 5 のシステムブロック図

【図 8】



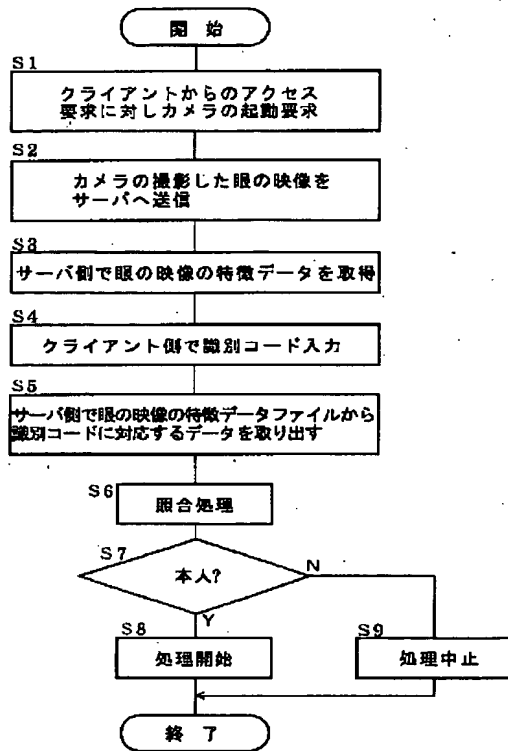
具体例 5 のシステム動作フローチャート

【図 9】



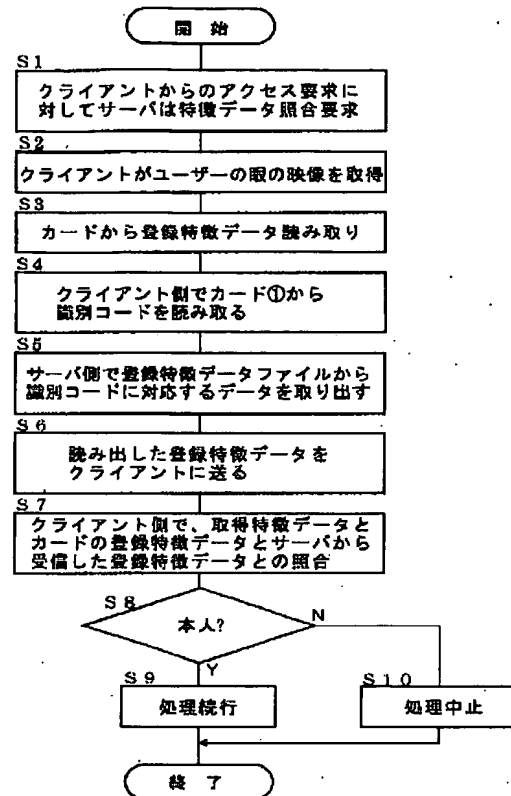
具体例 6 のシステムブロック図

【図10】



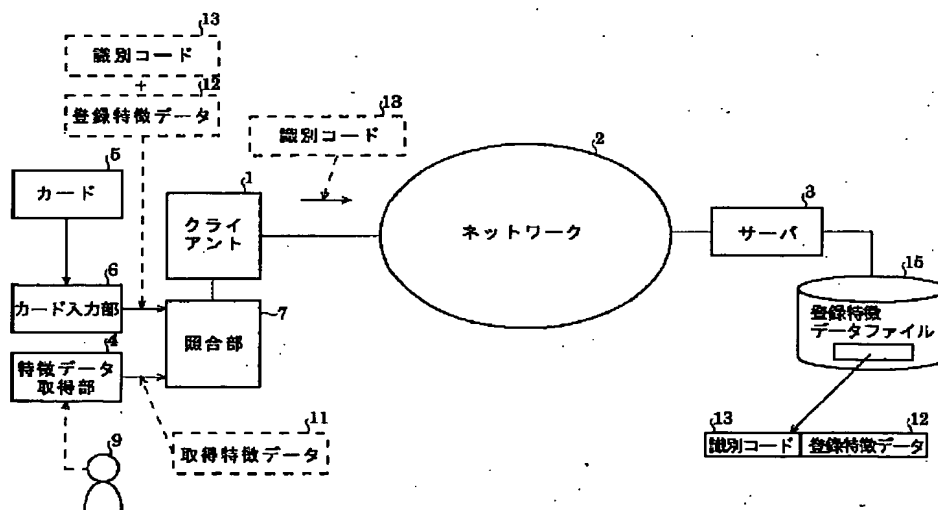
具体例6のシステム動作フローチャート

【図12】



具体例7のシステム動作フローチャート

【図11】



具体例7のシステムブロック図

フロントページの続き

(51)Int.Cl.⁶

G 0 6 T 7/00

識別記号

F I

G 0 6 F 15/62

4 6 5 A